МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП НАДВІРНЯНСЬКИЙ ФАХОВИЙ КОЛЕДЖ НАЦІОНАЛЬНО ТРАНСПОРТНОГО УНІВЕРСИТЕТУ

Дипломний проект

Тема: « Розроблення модуля шифрування інформації в каналах зв'язку на основі системи залишкових класів »

Виконавець: Луців Ю.М.
Керівник: Волинський О.І.

ВСТУП

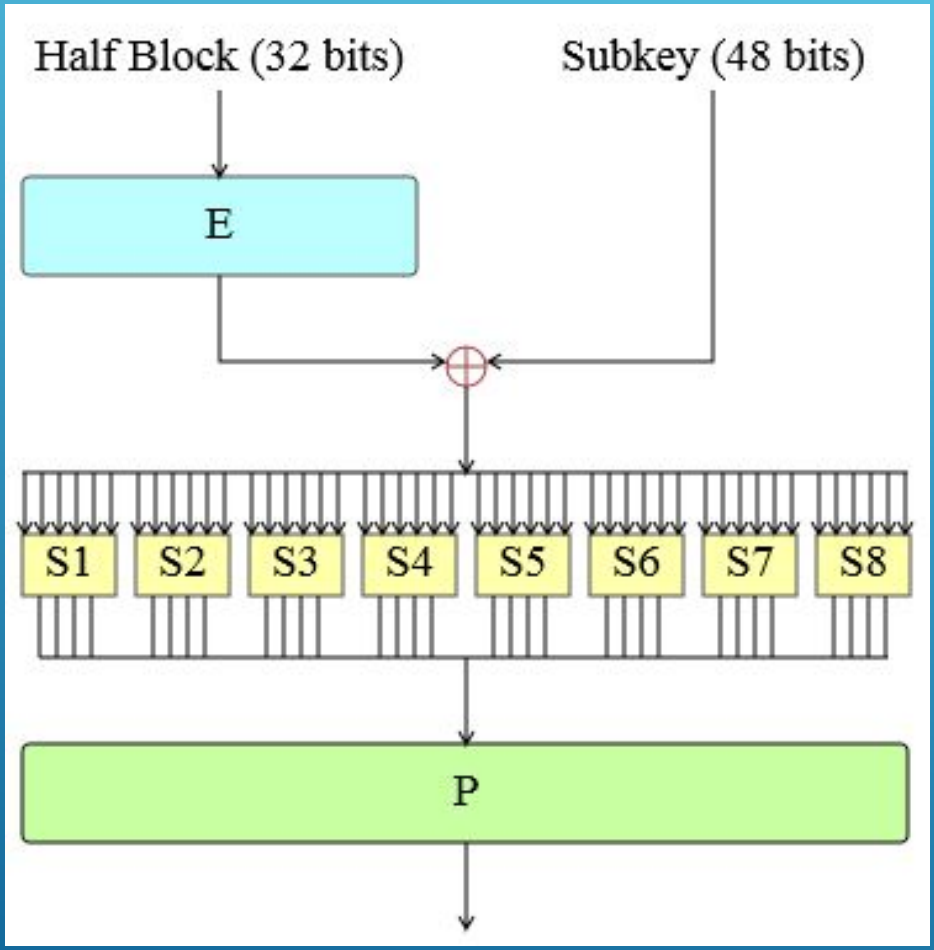
- У наш високо інтелектуальний час важко переоцінити важливість інформації. Саме тому актуальною темою для досліджень залишається її передача та захист. Зокрема, існує безліч шляхів передачі даних. Окремі з винайдених відійшли у небуття, а деякі залишились. При цьому актуалізується питання кодування інформації.

1. **Об’єкт проектування** – захист текстової інформації.
2. **Предмет проектування** – програмний модуль шифрування даних.
3. **Мета дипломного проекту** – розробка апаратно-програмного модуля шифрування даних для кодування інформації за рахунок представлення даних у системі залишкових класів.

Завдання проектування

1. Проаналізувати методи шифрування текстових даних.
2. Розробити структуру модуля шифрування даних.
3. Розробити простий та зручний інтерфейс модуля.
4. Реалізувати алгоритм шифрування роботи пристроїв які використовують для реалізації шифраторів на основі базису Крестенсона.

Рисунок 1.1 – Структура блоку шифрування DES



(Data Encryption Standard). DES є блочним шифром - дані шифруються блоками по 64 біти - 64 бітний блок явного тексту подається на вхід алгоритму, а 64-бітний блок шифрограми отримується в результаті роботи алгоритму. Крім того, як під час шифрування, так і під час дешифрування використовується один і той самий алгоритм (за винятком дещо іншого шляху утворення робочих ключів). Безпечність алгоритму базується на безпечності ключа.

Принципи побудови й схеми криптографічного захисту

Рисунок 2.1 – Загальна структура криптосистеми

На даному рисунку представлена криптологічна система.

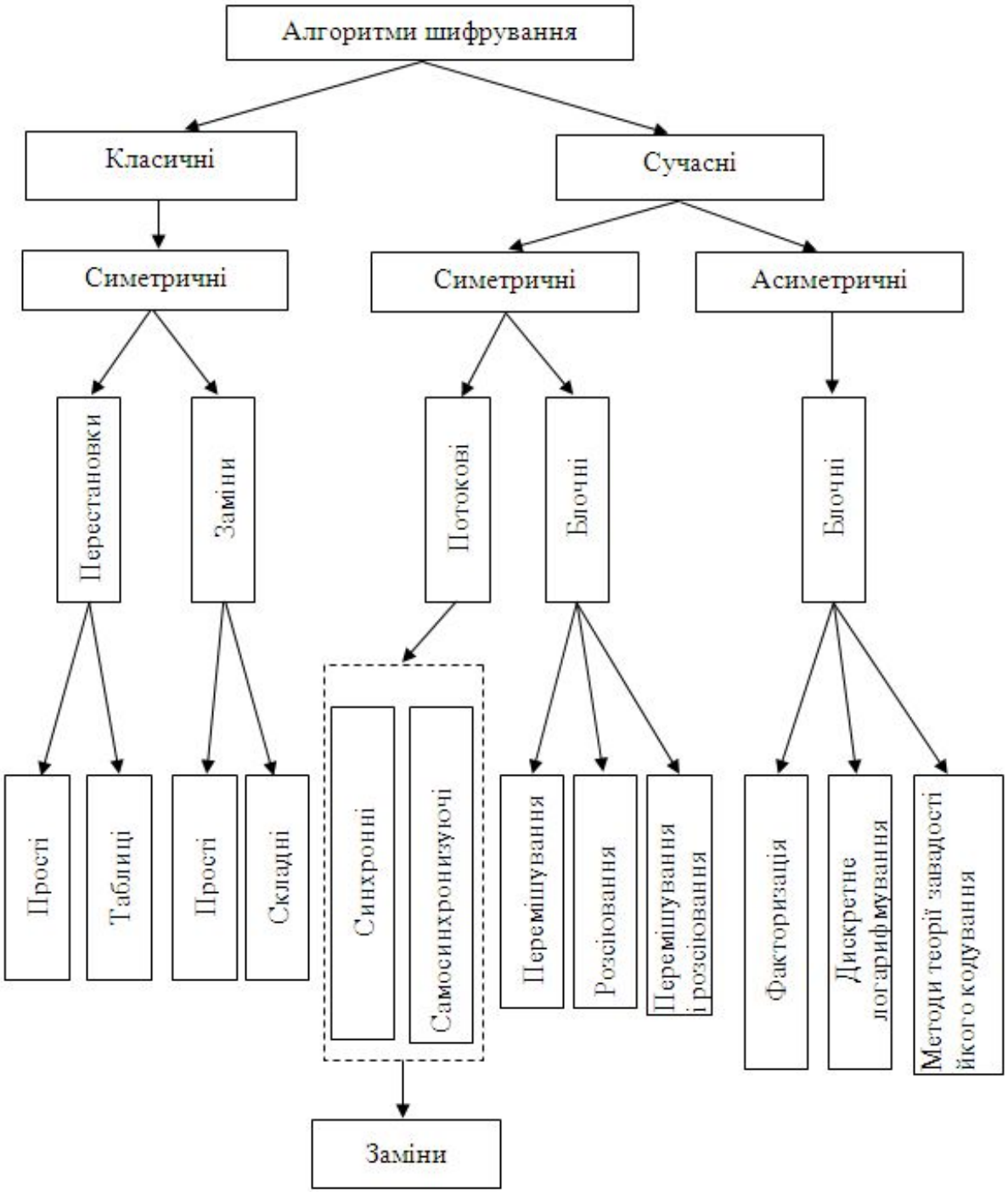


Рисунок 2.2 – Класифікація алгоритмів шифрування

Методи шифрування	Переваги	Недоліки
Симетричне шифрування	1) Висока швидкість шифрування. 2) Менша довжина ключа, ніж в асиметричному шифруванні. 3) Проста реалізація.	1) Публічна передача ключів, враховуючи велику ймовірність порушення секретності ключа. 2) Квадратична залежність числа ключів при великій кількості користувачів.
Асиметричне шифрування, або шифрування з відкритим ключем	1) Вирішена проблема розподілу ключів між користувачами, так як кожен користувач може згенерувати свою пару ключів сам, а відкриті ключі користувачів можуть вільно публікуватися. 2) Зникає квадратична залежність числа ключів від числа користувачів (2N та N(N-1)/2).	1) Повільніше ніж симетричне шифрування, оскільки при шифруванні і розшифрування використовуються досить ресурсомісткі операції. 2) Необхідність захисту відкритих ключів від підміни. 3) Немає математичних доказів незворотності використовуваних функцій.

Перетворення та арифметика в СЗК

N_k	b_1	b_2
0	0	0
1	1	1
2	0	2
3	1	3
4	0	4
5	1	0
6	0	1
7	1	2
8	0	3
9	1	4

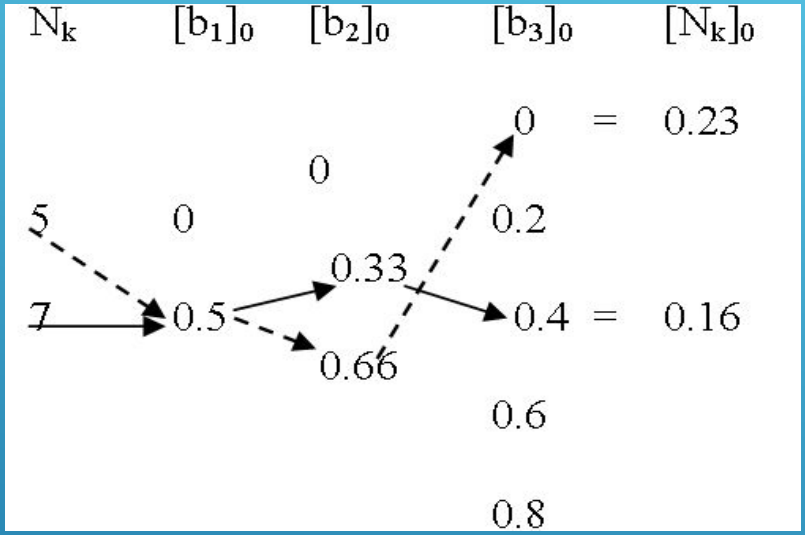
Таблиця 2.1 – Кодування чисел в цілочисельній формі СЗК.

N_k	$[b_1]_0$	$[b_2]_0$	$[b_3]_0$	$[N_k]_0$
0	0	0	0	0
1	0.5	0.333	0.2	0.033
2	0	0.666	0.4	0.066
3	0.5	0	0.6	0.1
4	0	0.333	0.8	0.133
5	0.5	0.666	0	0.166
6	0	0	0.2	0.2
7	0.5	0.333	0.4	0.233
…	…	…	…	…
29	0.5	0.666	0.8	0.966

Таблиця 2.3 – Перетворення векторів багатомірного дискретного простору залишків у одномірний дискретний простір Радемахера

N_k	$p_1=2$	$p_2=3$	$p_3=5$
0	0	0	0
1	1	1	1
2	0	2	2
3	1	0	3
4	0	1	4
5	1	2	0
6	0	0	1
…	…	…	…
20	0	2	0
…	…	…	…
28	0	1	3
29	1	2	4

Таблиця 2.2 – Представлення залишків в досконалій СЗК



2.3 Граф визначення $[N_{k2}]_0$

Операція міжбазисного перетворення може бути представлена у вигляді графа сумування нормалізованих значень залишків в заданій системі модулів. Наприклад: для двох чисел згідно таблиці 2.3 отримаємо їх коди у нормалізованій СЗК N_{k1}= (0,5;0,66;0), N_{k2}=(0,5;0,33;0,4) і, згідно графу на рисунку 2.3, отримуємо їх нормалізовані значення у системі модулів (2, 3, 5) $[N_{k1}]_0$= 0,16 і $[N_{k2}]_0$=0,23.

2.4 показана процедура міжбазисного перетворення Крестенсона-Радемахера на основі НСЗК.


b_i
p_1=3
p_2=5
p_3=7
p_4=8
p_5=11
p_6=13
0
0.0
0.0
0.0
0.0
0.0
0.0
1
0.1010101010101010101010
0.1100110011001100110011
0.1011011011011011011011
0.111
0.1010001011101000101010
0.0100111011000100111102 (mod1)0,0000000000000001
2
0.0101010101010101010101
0.1001100110011001100110
0.0110110110110110110110
0.110
0.0100010111010001011102
0.1001110110001001110202
3
0.0110011001100110011010
0.0010010010010010010010
0.101
0.1110100010111010001010
0.1110110001001110101103
4
0.0011001100110011001101
0.1101101101101101101102
0.100
0.1000101110100010111010
0.0011101100010011101004
5
0.1001001001001001001010
0.011
0.0010111010001011101005
0.1000100111011000100102 (mod1)0,0000000000000010105
6
0.0100100100100100100100
0.010
0.1101000101110100010106
0.1101100010011010111106
7
0.001
0,0111010001011101000107
0.0010011101100010011107
8
0.0001011101000101110108
0.0111011000100111010108
9
0.1011101000101110100009
0.1100010011011000010009
10
0.0101000101110100010510
0.0001001110110001001110
11
0.0110001001111100010011
12
0.1011000100111011000012

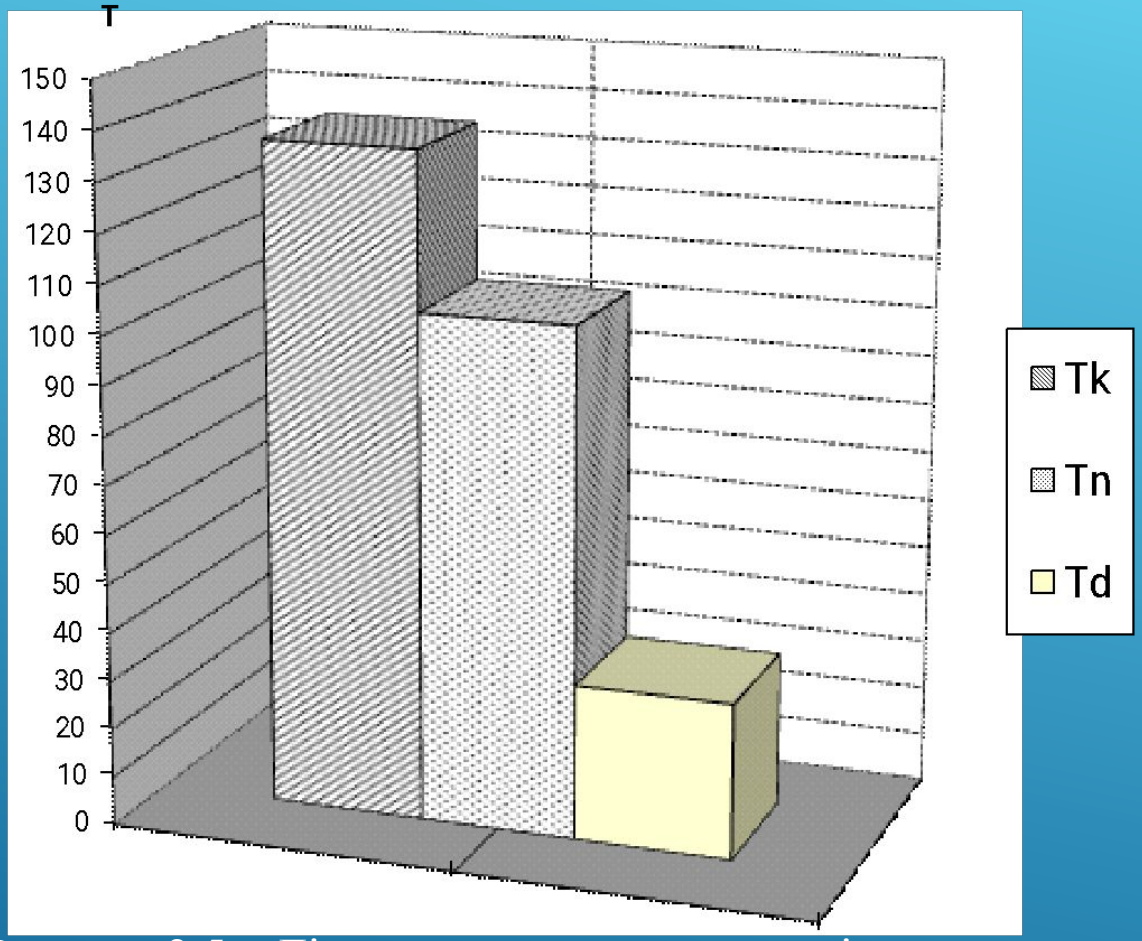


Рисунок 2.5 – Діаграма часової складності виконання перетворень цілочисельної, нормалізованої та досконалої форм СЗК

3. ПРОГРАМНО-АПАРАТНИЙ МОДУЛЬ ШИФРУВАННЯ ДАНИХ

Multisim – це унікальна можливість для інтерактивного створення принципових електричних схем і моделювання режимів їх роботи

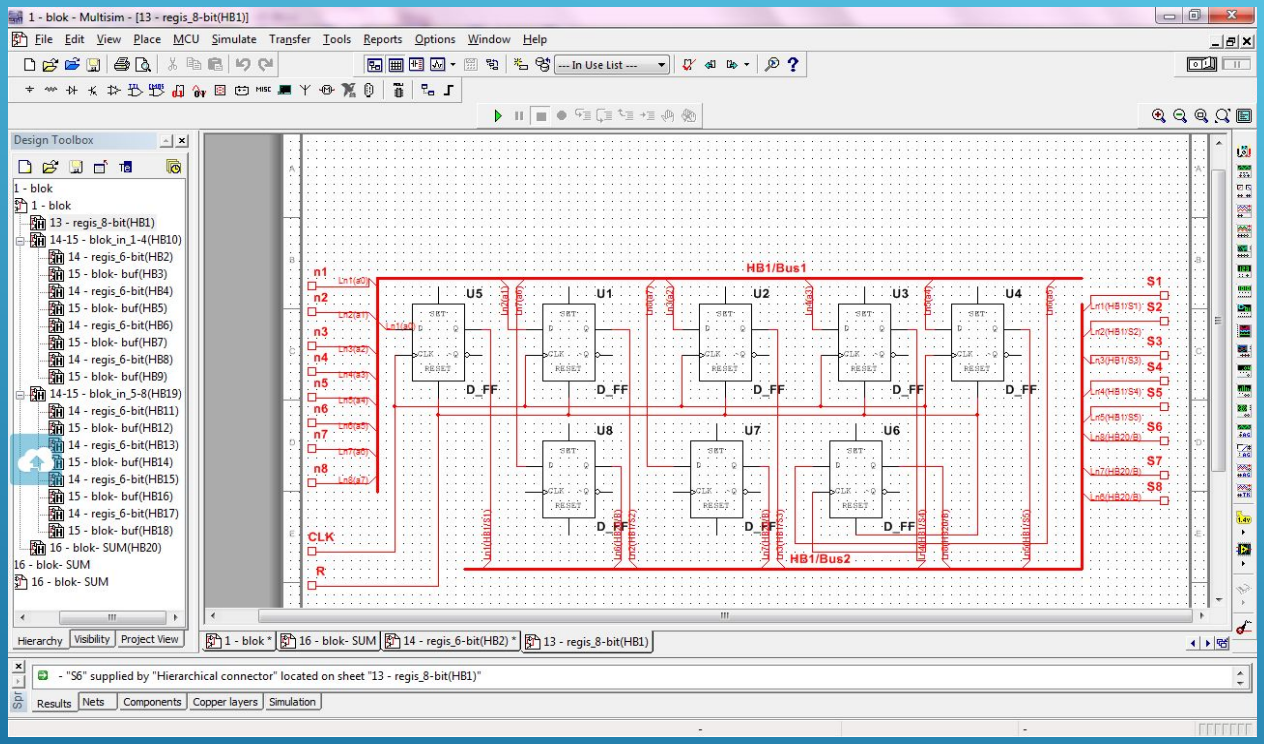
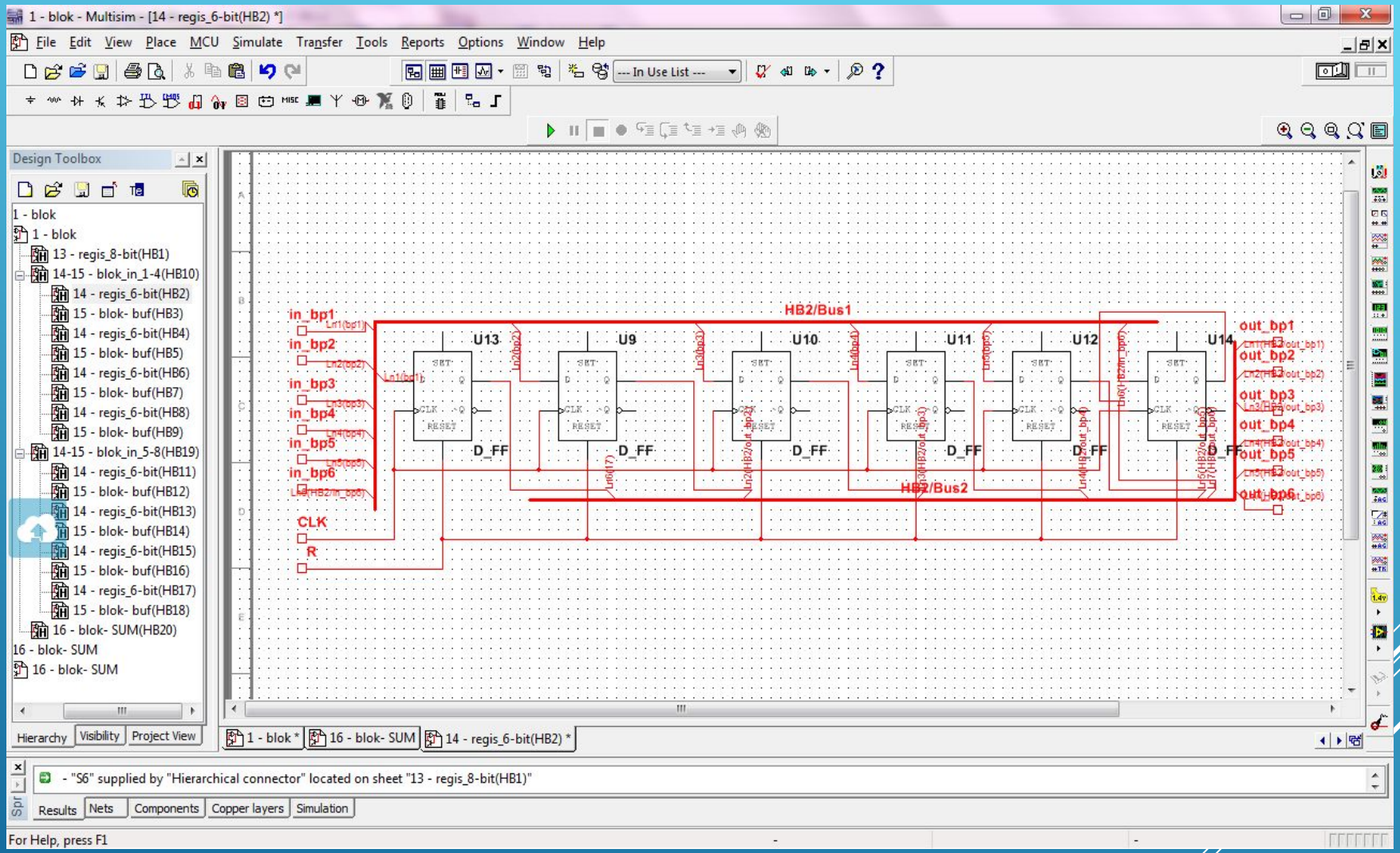
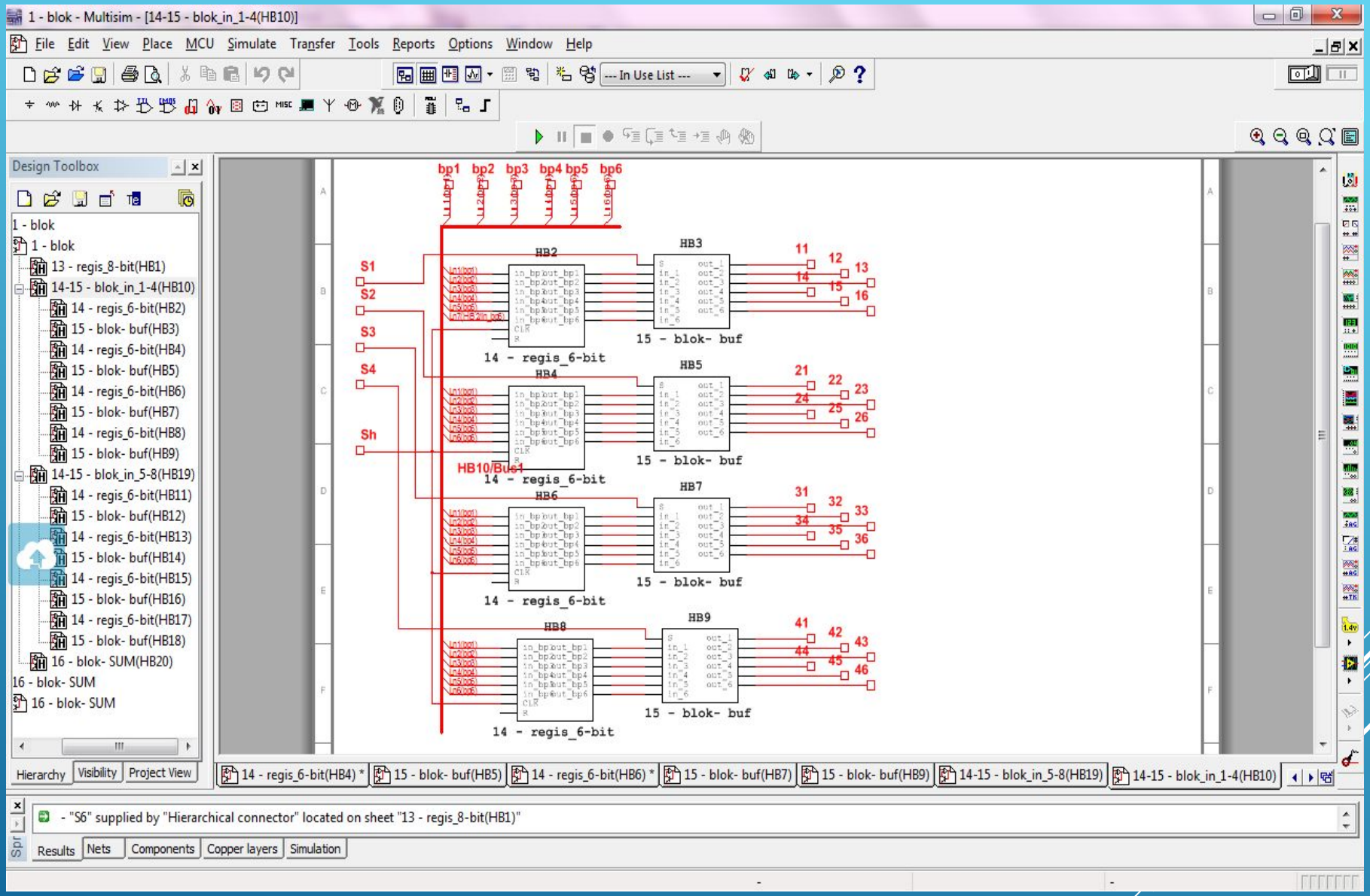


Рисунок 3.1 – Паралельний 8 розрядний регістр


1 - blok - Multisim - [14 - regis_6-bit(HB2) *]
File Edit View Place MCU Simulate Transfer Tools Reports Options Window Help
--- In Use List ---
Design Toolbox
1 - blok
1 - blok
13 - regis_8-bit(HB1)
14-15 - blok_in_1-4(HB10)
14 - regis_6-bit(HB2)
15 - blok- buf(HB3)
14 - regis_6-bit(HB4)
15 - blok- buf(HB5)
14 - regis_6-bit(HB6)
15 - blok- buf(HB7)
14 - regis_6-bit(HB8)
15 - blok- buf(HB9)
14-15 - blok_in_5-8(HB19)
14 - regis_6-bit(HB11)
15 - blok- buf(HB12)
14 - regis_6-bit(HB13)
15 - blok- buf(HB14)
14 - regis_6-bit(HB15)
15 - blok- buf(HB16)
14 - regis_6-bit(HB17)
15 - blok- buf(HB18)
16 - blok- SUM(HB20)
16 - blok- SUM
16 - blok- SUM
Hierarchy Visibility Project View
HB2/Bus1
HB2/Bus2
in_bp1
in_bp2
in_bp3
in_bp4
in_bp5
in_bp6
CLK
R
U13
U9
U10
U11
U12
U14
D_FF
out_bp1
out_bp2
out_bp3
out_bp4
out_bp5
out_bp6
1 - blok *
16 - blok- SUM
14 - regis_6-bit(HB2) *
- "S6" supplied by "Hierarchical connector" located on sheet "13 - regis_8-bit(HB1)"
Results Nets Components Copper layers Simulation
For Help, press F1


1 - blok - Multisim - [14-15 - blok_in_1-4(HB10)]
File Edit View Place MCU Simulate Transfer Tools Reports Options Window Help
Design Toolbox
1 - blok
1 - blok
13 - regis_8-bit(HB1)
14-15 - blok_in_1-4(HB10)
14 - regis_6-bit(HB2)
15 - blok- buf(HB3)
14 - regis_6-bit(HB4)
15 - blok- buf(HB5)
14 - regis_6-bit(HB6)
15 - blok- buf(HB7)
14 - regis_6-bit(HB8)
15 - blok- buf(HB9)
14-15 - blok_in_5-8(HB19)
14 - regis_6-bit(HB11)
15 - blok- buf(HB12)
14 - regis_6-bit(HB13)
15 - blok- buf(HB14)
14 - regis_6-bit(HB15)
15 - blok- buf(HB16)
14 - regis_6-bit(HB17)
15 - blok- buf(HB18)
16 - blok- SUM(HB20)
16 - blok- SUM
16 - blok- SUM
Hierarchy Visibility Project View
bp1 bp2 bp3 bp4 bp5 bp6
S1
S2
S3
S4
Sh
HB2
HB3
HB4
HB5
HB6
HB7
HB8
HB9
14 - regis_6-bit
15 - blok- buf
HB10/Bus1
14 - regis_6-bit(HB4) *
15 - blok- buf(HB5)
14 - regis_6-bit(HB6) *
15 - blok- buf(HB7)
15 - blok- buf(HB9)
14-15 - blok_in_5-8(HB19)
14-15 - blok_in_1-4(HB10)
- "S6" supplied by "Hierarchical connector" located on sheet "13 - regis_8-bit(HB1)"
Results Nets Components Copper layers Simulation

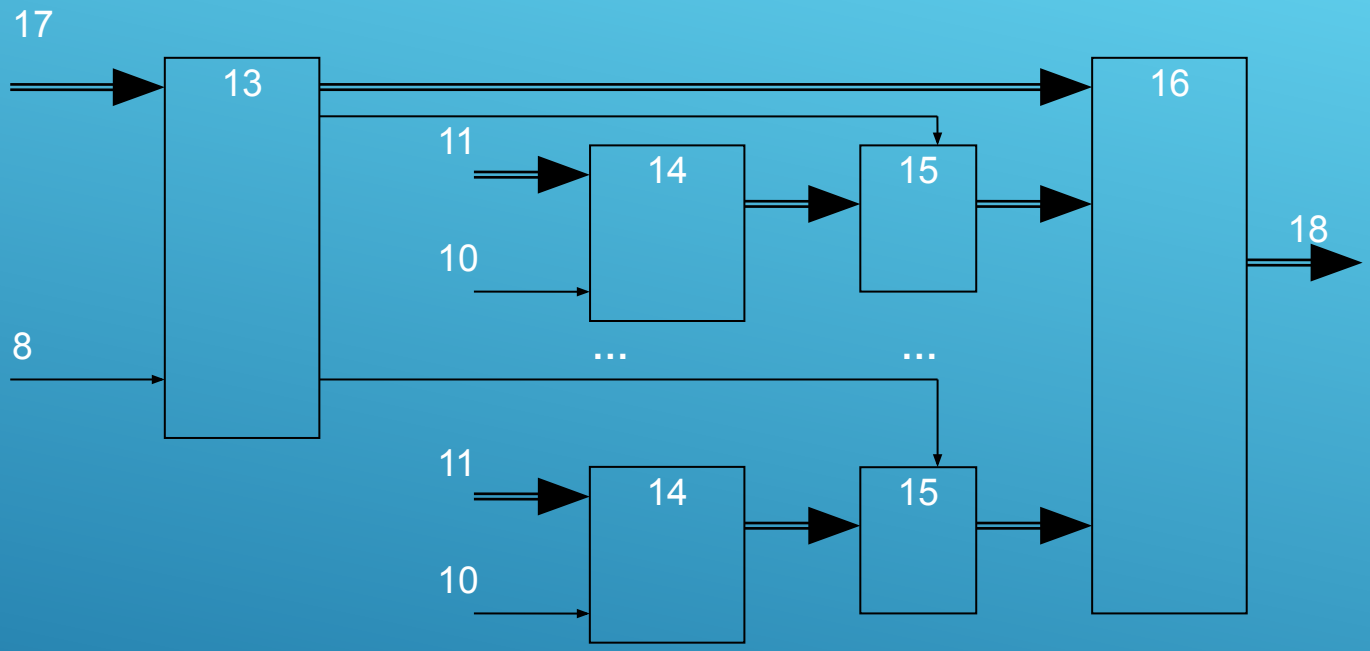


Рисунок 3.4 – Блок формування часткових залишків

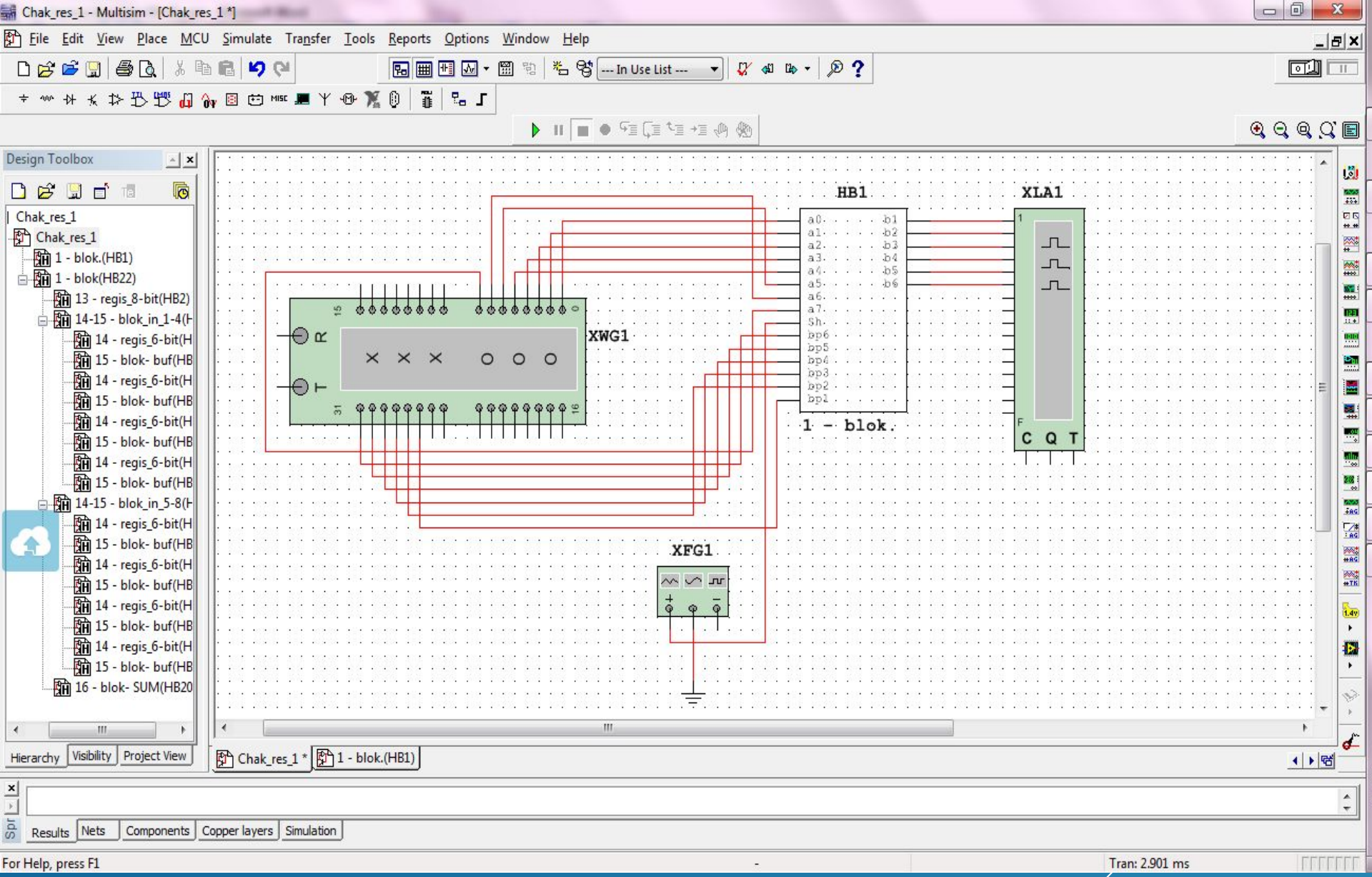


Рисунок 3.5 – Блоку формування проміжного залишку

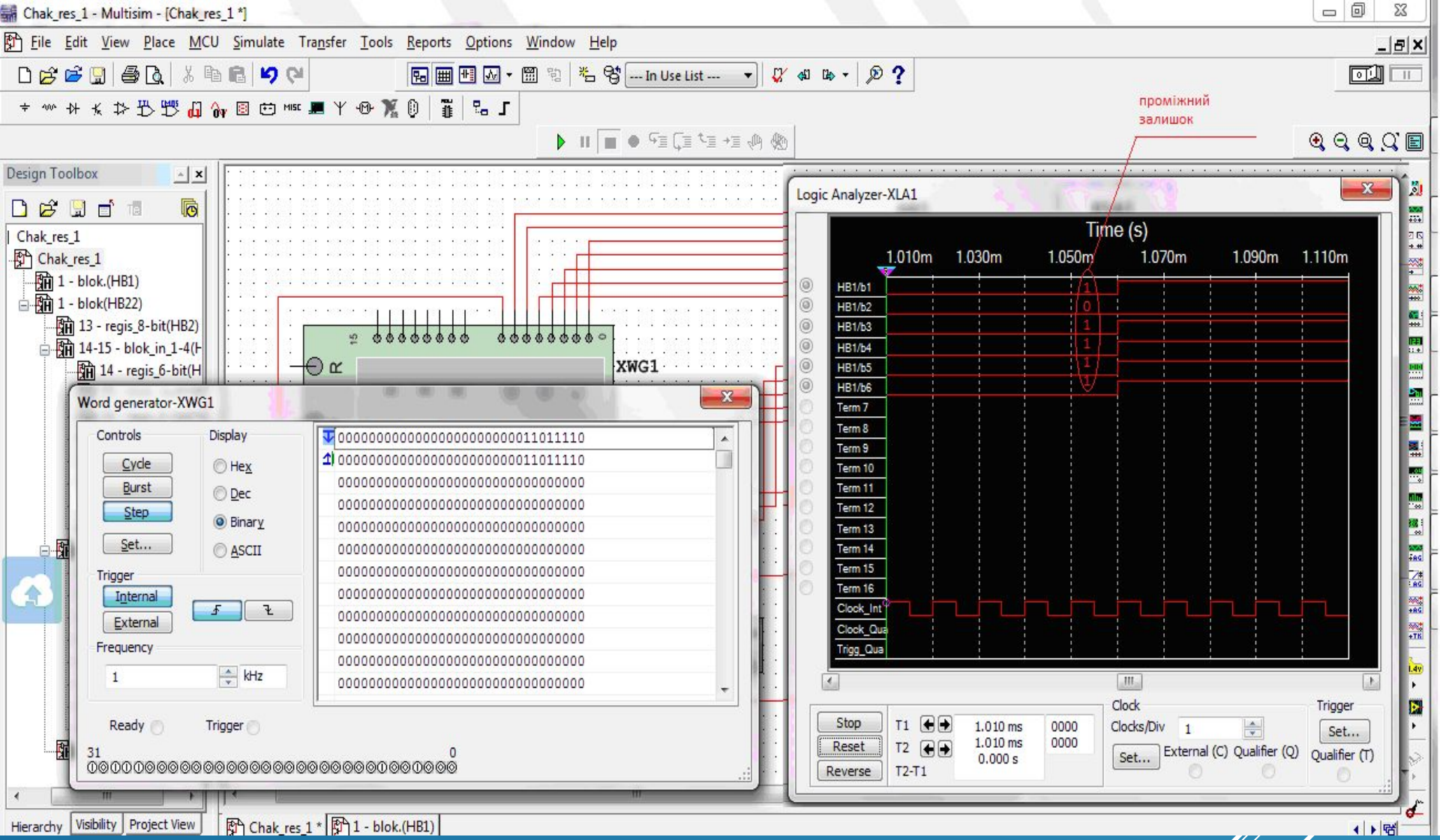


Рисунок 3.6 – Блоку формування проміжного залишку, результат роботи

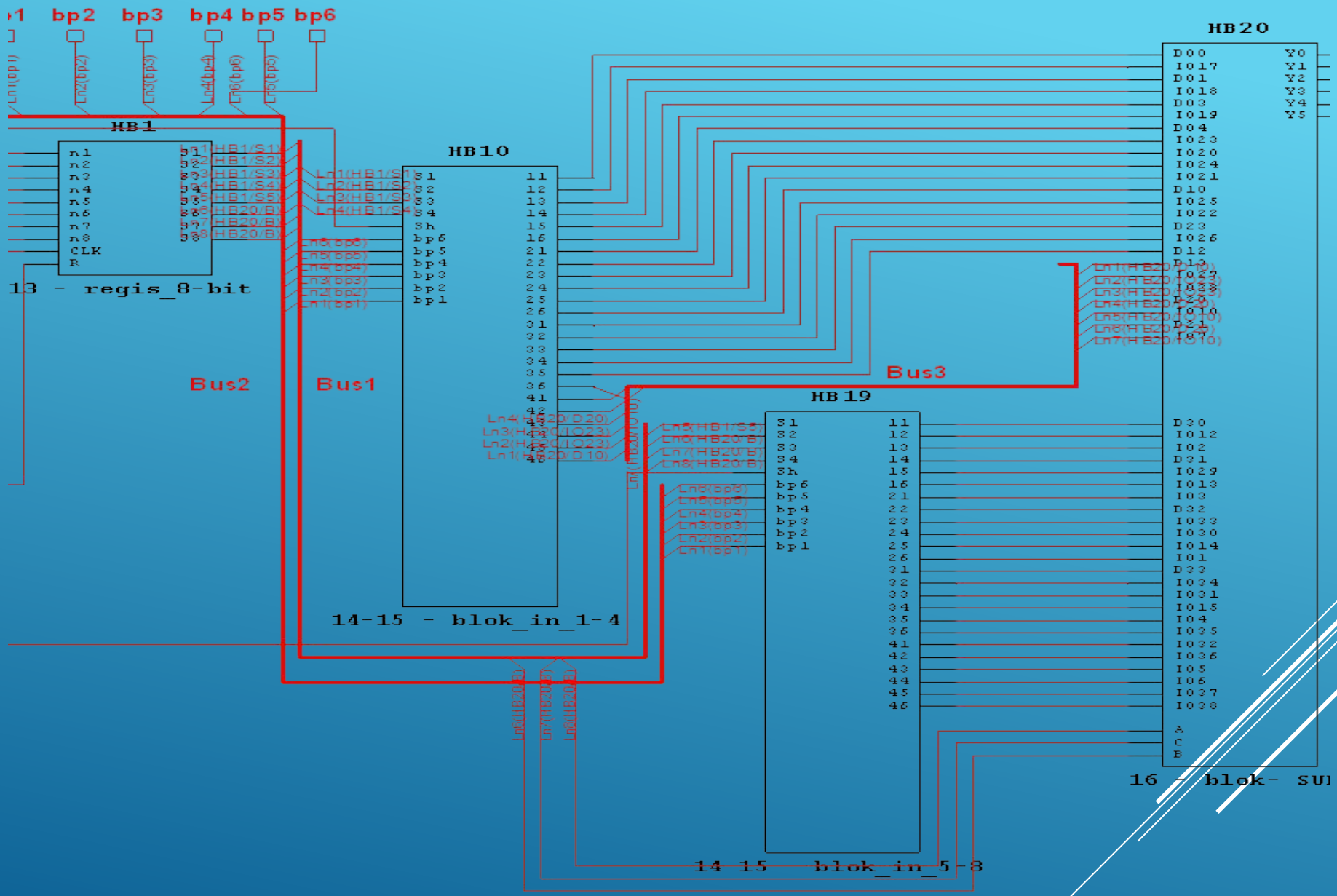


Схема електрична функціональна

ВИСНОВКИ

Проаналізовані причини появи методів захисту інформації, а також розглянуто термінологію і найбільш розповсюджені криптографічні стандарти. В результаті аналізу було встановлено, що перспективним напрямком досліджень захисту інформації є використання теоретико-числового базису Крестенсона

Досліджено та проаналізовано алгоритми роботи пристроїв які використовують для реалізації шифраторів на основі базису Крестенсона.

Розроблено та описано принцип роботи структурної схеми. Проаналізовано необхідні для реалізації структурні елементи та їх характеристики.

Дякую за увагу